**Załącznik nr 2**

**Rozmiar środowiska informatycznego (produkcyjne) Zamawiającego.**

|  |  |  |
| --- | --- | --- |
| **Obszar** | **Wolumen** | **Uwagi** |
| Elementy aktywne sieci | 300+ | Wykorzystywane marki urządzeń sieciowych: Cisco, Alcatel, Mikrotik, Dell, Fortinet, |
| Serwery wirtualne | Microsoft – 200+  Linux/Unix/Solaris – 50+ |  |
| Serwery fizyczne | ~75-100 |  |
| Stacje robocze | Stacje klienckie – 1600+  Thin clients – 300+ | w tym thin clients |
| Liczba lokalizacji spiętych MPLS | ~30 | Oddziały i Komory Przeładunkowe. |
| Ilość zdarzeń rejestrowanych dziennie | Średnio około 30 GB/dziennie, szczytowo ponad 48 GB dziennie. |  |
| Liczba źródeł do SIEM | Około 400 źródeł dla około 40 indeksów | Jeśli chodzi o indexy, co do metod to syslog i forwarder |

**Załącznik nr 3**

**Oświadczenie spełnienia wymagań dla podmiotu świadczącego usługi w zakresie bezpieczeństwa wynikające z Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa oraz Rozporządzenia z dnia 04 grudnia 2019 w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.**

**…………………………………………………..**

**……………………………………………………**

**(Nazwa i NIP Oferenta)**

W związku z prowadzeniem działalności z zakresu usług cyberbezpieczeństwa, niniejszym oświadczamy, że nasze Centrum Operacyjne Bezpieczeństwa (SOC) spełnia wszystkie wymagania określone w ustawie o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. oraz Rozporządzeniu Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo operatorów usług kluczowych.

Nasze SOC spełnia następujące wymogi prawne:

* + 1. Zarządzanie bezpieczeństwem informacji: Wdrożyliśmy i aktualizujemy system zarządzania bezpieczeństwem informacji zgodny z normą ISO/IEC 27001, obejmujący co najmniej świadczone przez nas usługi.
    2. Zapewnienie ciągłości działania: Zapewniamy ciągłość działania oraz wsparcie operatorom usług kluczowych w zakresie obsługi incydentów z czasem reakcji adekwatnym do charakteru świadczonych usług.
    3. Polityka działania zgodna z RFC 2350: Posiadamy i udostępniamy w języku polskim i angielskim deklarację polityki działania w zakresie zgodnym z dokumentem RFC 2350, zgodnie z zaleceniami Internet Engineering Task Force (IETF).
    4. Personel z odpowiednimi kwalifikacjami:
* Nasz personel posiada wymagane umiejętności w zakresie:
* Identyfikacji zagrożeń w systemach informacyjnych operatorów usług kluczowych,
* Analizy szkodliwego oprogramowania i jego wpływu na systemy,
* Wykrywania przełamań lub ominięcia zabezpieczeń oraz prowadzenia analizy powłamaniowej,
* Zabezpieczania dowodów powłamaniowych i analizowania skutków incydentów.
  + 1. Zabezpieczenia fizyczne:

Przeprowadziliśmy analizę ryzyka oraz wdrożyliśmy odpowiednie środki techniczne i fizyczne, obejmujące:

* Zabezpieczenie pomieszczeń wykorzystywanych do świadczenia usług SOC,
* Systemy kontroli dostępu, sygnalizacji pożarowej oraz alarmy chroniące przed nieuprawnionym dostępem.
  + 1. Sprzęt i narzędzia techniczne:
* Dysponujemy odpowiednim sprzętem komputerowym oraz narzędziami informatycznymi, umożliwiającymi rejestrację incydentów, analizę szkodliwego oprogramowania oraz badanie odporności systemów informacyjnych na zagrożenia.
* Zobowiązujemy się do dalszego przestrzegania przepisów prawnych oraz utrzymania zgodności operacyjnej i technicznej z wymogami wynikającymi z ustawy oraz rozporządzenia, oraz z wprowadzanych zmian aby zapewniać najwyższy poziom bezpieczeństwa naszym klientom.

**Data:**  
**Podpis osoby odpowiedzialnej:**

**Załącznik nr 4**

**Potwierdzenie spełnienia warunku – w formie oświadczenia o spełnienia warunku świadczeniu co najmniej 5 pełnowymiarowe usługi SOC o łącznej wartości minimum 1.500.000,00 zł rocznie.**

**…………………………………………………..**

**……………………………………………………**

**(nazwa i nip Oferenta)**

Niniejszym oświadczamy, że nasza organizacja spełnia warunek świadczenia co najmniej 5 pełnowymiarowych usług SOC (Security Operations Center), których łączna wartość wynosi **minimum 1.500.000,00 zł rocznie netto**. Usługi te są realizowane zgodnie z najwyższymi standardami bezpieczeństwa, na rzecz dużych klientów, zapewniając kompleksowe wsparcie w zakresie monitorowania i zarządzania bezpieczeństwem IT.

**Data:**  
**Podpis osoby upoważnionej:**

**Załącznik nr 5**

### **Oświadczenie o spełnieniu warunku zatrudnienia analityków bezpieczeństwa**

**…………………………………………………..**

**……………………………………………………**

**(Nazwa i NIP Oferenta)**

Niniejszym oświadczamy, że nasza organizacja spełnia warunek zatrudnienia **co najmniej 10 osób** na stanowiskach analityków bezpieczeństwa I, II oraz III linii wsparcia SOC (Security Operations Center), którzy posiadają specjalistyczną wiedzę i kwalifikacje wymagane do realizacji usług SOC.

Oświadczamy, że wszyscy zatrudnieni analitycy spełniają wymogi dotyczące kompetencji oraz posiadają niezbędne certyfikaty wymagane do realizacji swoich obowiązków.

### **Zanonimizowane zestawienie pracowników SOC**

| **Lp.** | Stanowisko, odpowiedzialność, linia wsparcia (I, II, III) | Doświadczenie zawodowe (lata) ogólnie, u Dostawcy, forma zatrudnienia | Posiadane certyfikaty |
| --- | --- | --- | --- |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| 11 |  |  |  |
| 12 |  |  |  |
| 13 |  |  |  |
| 14 |  |  |  |
| 15 |  |  |  |

**Objaśnienia do wypełnienia:**

Warunek zatrudnienia określający, że wykonawca musi zatrudniać co najmniej 10 osób – analityków bezpieczeństwa I, II i III linii wsparcia SOC, obejmuje zarówno osoby zatrudnione na podstawie **umowy o pracę**, jak i osoby współpracujące na podstawie innych form zatrudnienia, takich jak **umowy B2B, umowy zlecenie** czy inne umowy cywilnoprawne.

W celu spełnienia tego warunku, do liczby 10 osób mogą być wliczone:

1. **Pracownicy etatowi (umowa o pracę)**:Osoby zatrudnione na pełen etat lub w niepełnym wymiarze czasu pracy, które realizują zadania związane z analizą bezpieczeństwa w ramach struktur SOC, z przypisanymi obowiązkami w zakresie monitorowania zagrożeń, analizą incydentów oraz reagowaniem na zagrożenia.
2. **Współpracownicy na zasadach umowy B2B**:Specjaliści świadczący usługi na rzecz SOC w oparciu o **kontrakt biznesowy** (B2B), którzy formalnie prowadzą działalność gospodarczą i realizują zadania w zakresie bezpieczeństwa IT zgodnie z zakresem swoich kompetencji. Zatrudnienie takie ma charakter outsourcingu, ale obejmuje kluczowe działania SOC i jest zgodne z wymaganiami.
3. **Osoby pracujące na podstawie umów zlecenia**: W ramach tego warunku mogą być uwzględnieni także **zleceniobiorcy**, którzy świadczą usługi w formie zleceń lub kontraktów na określony zakres prac związanych z SOC. Zleceniobiorcy wykonują zadania z zakresu monitorowania i analizy zagrożeń zgodnie z ustalonym zakresem obowiązków.

### Kluczowe aspekty:

* Warunek zatrudnienia obejmuje **różnorodne formy współpracy**, nie ograniczając się wyłącznie do umów o pracę.
* Ważne jest, aby każda z tych osób spełniała wymagania dotyczące kompetencji, posiadała odpowiednią wiedzę i kwalifikacje, które są zgodne z obowiązkami wynikającymi z pracy na różnych liniach wsparcia SOC.

**Data:**  
**Podpis osoby upoważnionej:**

**Załącznik nr 6**

**Oświadczenie**

**…………………………………………………..**

**……………………………………………………**

**(nazwa i nip Oferenta)**

W związku z ze złożoną ofertą, niniejszym oświadczamy, że ofertowany SOC zapewnia monitoring oraz wsparcie telefoniczne i e-mailowe w trybie 24/7/365.

Zakres świadczonych usług obejmuje:

* Monitoring bezpieczeństwa – całodobowe, nieprzerwane monitorowanie infrastruktury informatycznej Zamawiającego w celu wykrywania i reagowania na zagrożenia bezpieczeństwa.
* Wsparcie techniczne – całodobowe wsparcie telefoniczne i e-mailowe dla zgłoszeń związanych z incydentami bezpieczeństwa, dostępne przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.

Potwierdzamy, że nasz zespół Security Operations Center (SOC) jest gotowy do natychmiastowego reagowania na zgłoszenia i incydenty zgodnie z ustalonymi procedurami które będą zawarte w umowie.

**Data:**  
**Podpis osoby upoważnionej:**

**Załącznik nr 7**

**Podmioty wchodzące do Grupy Kapitałowej Farmacol:**

* Farmacol-Logistyka Sp. z o.o. – Katowice
* Silesian Pharma Sp. z o.o. – Katowice
* PZF Cefarm Kielce S.A. – Kielce
* PZF Cefarm Warszawa S.A. – Warszawa
* PZF Cefarm Szczecin S.A. – Szczecin
* Cefarm Białystok S.A. – Białystok
* Nasza Apteka Sp. z o.o. – Nowy Sącz
* Apteka Tęczowa Sp. z o.o. – Szczecin
* Apteka Helios Sp. z o.o. – Szczecin
* Firma Zdrowie Sp. z o.o. – Bytom
* Kwiaty Polskie Sp. z o.o. – Łódź
* Pod Orlikiem Sp. z o.o. – Ustrzyki Dolne
* PZF Cefarm Warszawa S.A. Sp. jawna – Brzozów
* Apteka Milenium Sp. z o.o. – Brzesko
* Pharma Flos Sp. z o.o. – Tychy
* Best Farm Sp. z o.o. – Łódź
* Farmax Sp. z o.o. – Łódź
* Farmacore Sp. z o.o. – Wrocław